ijergs
Open Access
International Journal of Engineering Research and Generic Science (IJERGS)
Available Online at www.ijergs.in
ISSN: 2455 - 1597
Volume -2, Issue-6, November - December 2016, Page No. 15 - 20

A Proposed Scenario on DDOS Attacks in Cloud Computing

Neha Kachchhawat[1], Neelima Bhardwaj[2]

[1]Computer Science & Engineering, Arya Group of Colleges, Jaipur, Rajasthan, India

[2]Assistant Professor, Computer Science & Engineering, AIET, Jaipur, Rajasthan, India

E-Mail Id: nehak2109@gmail.com

Abstract

Cloud is becoming a prevalent computing podium. Cloud computing is one of the arising technique in which massive amount of data, storage and services are available over the internet. The interesting advantage of cloud computing medium is the users only have to pay for that only what they actually use. A Dos attacks as its name suggests is openly an attack by an attacker to disable the availability of resources for a network, application or services so that authorize user can not earn access. Now a days the Denial of service attacks are the widely spread issue faced by various internet service providers (ISP's). Denial of service attacks have become a major threat to current computer network. Denial of service attacks is dangerous to networks as it delays genuine users from accessing the resources. This paper highlights various denial of service attack detection method in private cloud environment.

Keywords: Cloud Computing , DoS Attack, PDA, IP packets, D- Ward, ARIMA, CUSUM, SPUNNID, MULTOPS, EaaS

1. Introduction

Cloud computing is also known as on-demand computing. This computing is a kind of completely internet based computing which provides shared processing resources and data to computers and other devices on demand. Due to this competency to apportionment earthly cloud computing becomes more popular day by day. An internet is widely used in every aspect of our daily lives, it is become a demanding resource whose disruption has serious indications. Blocking availability of an internet service may imply large financial losses, as in case of an attack the prevented users from having steady connectivity to major e-commerce web sites such as yahoo, Amazon, eBay, E*Trade, Buy.com,ZDnet and CNN(Sandoval and Wolverton 2000) [3]. A denial of service attack on a network could pick one of three possible forms. A venomous party (a.k.a. the attacker) could cause the network not to dispatch messages it should be sending in order to offer service to a subset or all of its clients. On the other side of the spectrum, the network could be caused to dispatch messages, which it should not be dispatching. By far the most common form of DoS in today's networks is causing redundant bogus traffic (a.k.a. flooding the network) in the charge of a particular server, which in the end will prohibit consistent users from receiving the service they could otherwise be accepting from that server. Typical aims of DoS attack are, by sending large traffic volume consuming the bandwidth, Consume limited available resources by sending specific type of packets, Crash or overload the network by flooding packets [1]. Distributed denial-of-service attacks (DDoS) pose an immense threat to the Internet, and consequently many defense mechanisms have been proposed to combat them. Attackers constantly modify their tools to bypass these security systems, and researchers in turn modify their approaches to handle new attacks[4]. For considerable network operators, DoS attack is expensive but governable. The world's considerable Internet service providers and destination websites govern DoS attacks by over-provisioning (maintaining more servers and connectivity than they generally need to cope with peak loads due to legitimate traffic or DDoS) and by monitoring and rapidly responding to attacks using a set of best practices and tools. Operators of major networks and major websites often interact with one another through closed mailing lists, helping each other fend off attacks.

2. Essential Characteristics of Cloud Computing

There are five essential characteristics of Cloud Computing[2]:

- *On-demand self-service:* A user can provision computer resources without the need for interaction with cloud service provider personnel**.**
- *Broad network access:* Access to resources in the cloud is available over the network using standard methods in a manner that provides platform independent access to clients of all types. This includes a mixture of heterogeneous operating systems, and thick and thin platforms such as laptops, mobile phones, and Personal Digital Assistant (PDA).

- *Resource pooling:* A cloud service provider creates resources that are pooled together in a system that supports multi-tenant usage.
- *Rapid elasticity*: Resources can be rapidly and elastically provisioned. The system can add resources by either scaling u systems (more powerful computers) or scaling out systems (more computers of the same king), and scaling can be automatic or manual.
- *Measured service:* The use of cloud system resources is measured, audited, and reported to the customer based on a metered system. A client can be charged based on a known metric such as amount of storage used, number of transactions, network I/O or bandwidth, amount of processing power used, and so forth.

3. DoS Attack

Denial of Service attacks is constructed to consume available resources so that authorized users are unable to use the resources and are therefore "Denied Service". In a computer network environment the main resources are CPU, memory and bandwidth.

- By consuming CPU resources a DoS attack can prevent a network device from responding to managementrequests processing packets, effectively locking up the device.
- By consuming memory resources a DoS attack can prevent a network device from processing packets, effectively locking up the device.
- By consuming bandwidth resources a DoS attack can reduce the speed and volume of the legitimate network traffic.

A denial of service (DoS) attack is a malicious try to make a server or a network resource unavailable to users, usually by temporarily interrupting or suspending the services of a host connected to the Internet. Resources targeted in a DoS attack can be a specific computer, a port or service on the goaled system, an entire network, a component of a given network any system component.

There can be two different forms of Denial of Service attacks based on where is the origin of the attack being generated at:

- "Normal" DoS attacks are start to generat by a single host (or small number of hosts at the same location). The only actual way for DoS attacks to impose an original threat is to exploit some software or design flaw. Such flaws can include, for example, wrong implementations of the IP stack, which crash the whole host when receiving a non-standard IP packet (for example ping-of-death). Such an attack would generally have lower volumes of data.
- DDoS (Distributed Denial of Service) attacks would, usually, be generated by a high number of hosts. These hosts might be "zombies" , who were planted on remote hosts and have been waiting for the command to "attack" a victim. It is quite common to see attacks created by hundreds of hosts, creating hundreds of megabits per second floods.

4. DoS Attack Detection Methods in Private Cloud Environment

The four major classes of DoS Detection methods are:

- **Statistical Approaches**

Statistical properties of normal and attack patterns can be exploited for detection of DDoS attacks. Generally a statistical model for normal traffic is stated and then a statistical inference test is applied to determine if a new instance belongs to this model. Instances that do not conform to the learnt model, based on the applied test statistics, are classified as anomalies.

Chen et al. [5] developed a distributed change point (DCP) detection architecture using Change Aggregation Trees (CATs). The non-parametric "Cumulative Sum (CUSUM)" approach was adapted to describe the distribution of pre-change or post-change network traffic. When a DDoS flooding attack was being launched, the cumulative deviation was noticeably higher than random fluctuations. The CAT mechanism was designed to work at the router level to detect

abrupt changes in traffic flows. The domain server used the traffic change patterns detected at attack-transit routers to construct the CATs, which represent the attack flow pattern.

A very well-known DDoS defense scheme called D-WARD is presented in [6]. D-WARD identifies an attack based on continuous monitoring of bidirectional traffic flows between the network and the rest of the Internet and by periodic deviation analysis with the normal flow patterns. Mismatched flows are rate limited in proportion to their aggressiveness. DWARD not only offers a good detection rate but also reduces DDoS attack traffic significantly. It uses a predefined model for normal traffic to detect anomalies in the two-way traffic statistics for each peer. If it identifies a DDoS attack, it imposes a rate limit on the suspicious outgoing flow for the peer. Next, D-WARD observes the traffic for either confirmation of the attack or refutation. If the attack is confirmed, D-WARD further controls the rate limit. However, if refuted, it gradually allows increased traffic rate.

Zhang et al. [7] proposed a prediction method for the available service rate of a protected server by applying the Auto Regressive Integrated Moving Average (ARIMA) model. The authors have used available service rates to qualify the server's availability to detect DDoS attacks. Their prediction method divides server resources into CPU time, memory utilization and networking buffer. Based on the prediction, abnormal detection technology is used to analyze the consumption of server resources to predict whether the server is under DDoS attack.

Peng et al. [8] described a novel approach to detect bandwidth attacks by monitoring the arrival rate of new source IP addresses. The detection scheme is based on an advanced non-parametric change detection scheme, Cumulative Sum (CUSUM).

- **Soft Computing Methods**

Learning models, such as neural networks, radial basis functions and genetic algorithms are increasingly used in DoS attack detection because of their ability to classify intelligently and automatically. Soft computing is a general term for explaining a set of optimization and processing techniques that are tolerant of imprecision and uncertainty.

Jalili et al. [9] introduced a DDoS attack detection system called Unsupervised Neural Net based Intrusion Detector(SPUNNID) based on a statistical pre-processor and unsupervised artificial neural net. They have used statistical pre-processing to extract features from the traffic, and an unsupervised neural net to analyze and classify traffic patterns as either a DDoS attack or normal.

A method presented in [10] detects DDoS attacks based on a fuzzy estimator using mean packet inter-arrival times. It detects the suspected host and traces the IP address to drop packets within 3 second detection windows. Wu et al. [11] proposed to detect DDoS attacks using decision trees and grey relational analysis. The detection of the attack from the normal situation is viewed as a classification problem. The authors have used 15 attributes, which not only monitor the incoming/outgoing packet/byte rate, but also compile the TCP, SYN, and ACK flag rates, to describe the traffic flow pattern. The decision tree technique is applied to develop a classifier to detect abnormal traffic flow. A novel traffic

pattern matching procedure has also been used to identify traffic flow similar to the attack flow and to trace back the origin of an attack based on this similarity.

- **Knowledge based Methods**

In knowledge-based approaches, network events are checked against predefined rules or patterns of attack. In these approaches, general representations of known attacks are formulated to identify actual occurrences of attacks. Examples of knowledge-based approaches include expert systems, signature analysis, self organizing maps, and state transition analysis.

Gil and Poletto[12] introduced a heuristic along with a data structure called MULTOPS (Multi-Level Tree for Online Packet Statistics), that monitor certain traffic characteristics which can be used by network devices such as routers to detect and eliminate DDoS attacks. MULTOPS is a tree of nodes that contains packet rate statistics for subnet prefixes at different aggregation levels. Expansion and contraction of the tree occurs within a pre-specified memory size. A network device using MULTOPS detects ongoing bandwidth attacks by the presence of a significant and disproportional difference between packet rates going to and coming from the victim or the attacker.

Thomas et al. [13] presented an approach to DDoS defense called NetBouncer and claimed it to be a practical approach with high performance. The author's approach relies on distinguishing legitimate and illegitimate use and ensuring that resources are made available only for legitimate use. NetBouncer allows traffic to flow with reference to a long list of proven legitimate clients. If packets are received from a client (source) not on the legitimate list, a NetBouncer device proceeds to administer a variety of legitimacy tests to challenge the client to prove its legitimacy. If a client can pass these tests, it is added to the legitimacy list and subsequent packets from the client are accepted until a certain legitimacy window expires.

Wang et al. [14] presented a formal and methodical way of modeling DDoS attacks using Augmented Attack Tree (AAT), and discussed an AAT-based attack detection algorithm. This model explicitly captures the particular subtle incidents triggered by a DDoS attack and the corresponding state transitions from the view of the network traffic transmission on the primary victim server. Two major contributions of this paper are: (1) an AAT-based DDoS model (ADDoSAT), developed to assess potential threat from malicious packets on the primary victim server and to facilitate the detection of such attacks; (2) an AAT-based bottomup detection algorithm proposed to detect all kinds of attacks based on AAT modeling.

Limwiwatkul et al. [15] proposed to discover DDoS attack signatures by analyzing the TCP/IP packet header against well-defined rules and conditions, and distinguishing the difference between normal and abnormal traffic. The authors mainly focussed on ICMP, TCP and UDP flooding attacks.

- **Data Mining and Machine Learning Techniques**

Chen et al. [16] presented a comprehensive framework for DDoS attack detection known as DDoS Container. It uses a network based detection method to overcome complex and evasive types of DDoS attacks. It works in inline mode to inspect and manipulate ongoing traffic in real time. By continuous monitoring of both DDoS attacks and legitimate applications, DDoS Container covers stateful inspection on data streams and correlates events among different sessions. It proactively terminates the session when it detects an attack.

Rahmani et al. [17] discussed a joint entropy analysis of multiple traffic distributions for DDoS attack detection. The authors have observed that the time series of IPflow numbers and aggregate traffic sizes are strongly statistically dependant. The occurrence of an attack affects this dependence and causes a rupture in the time seriesfor joint entropy values. Experimental results showed that this method could lead to more accurate and effective DDoS detection.

Xiang et al. [18] proposed two new information metrics: (i) generalized entropy metric and (ii) information distance metric, to detect low rateDDoS attacks. The attack is identified by measuring the distance between legitimate traffic and attack traffic.

Francois et al. [19] presented a method called FireCol based on information theory for early detection of flooding DDoS attacks. FireCol is comprised of an intrusion prevention system (IPS) located at the Internet service provider (ISP) level. The Intrusion Prevention Systems (IPS) form virtual protection rings around the hosts to defend and collaborate by exchanging selected traffic information.

5. Conclusion

Cloud Computing revolutionize the way how Internet is used by providing everything as a service (EaaS) on pay per usage basis. Even though cloud offers a multitude of benefits to individuals and organizations, cloud is under high risk of attack and one such attack that can cause a major breach in security is DoS or DDoS attack. Distributed Denial of Services attack present biggest challenges to the researchers in the field of network security. It has already taken a heavy toll on many Internet based service providers in the world. There have been significant amount of work to tackle such DoS attack with different kinds of detection methods. In this paper, we have studied four major DoS detection approaches that are being considered by the experts in this field. Perhaps it will be a hard task to discuss each and every previously published work in this field. That's why we have kept the scope of the paper limited to just categorizing the existing approaches.

6. References

[1]. Nagaraju kilari Department of Computer Science, Garden City College, Dr. R. Sridaran Marwadi Education Foundation's Group of Institutions,–" An Overview of DDoS Attacks in Cloud Environment" International Journal of Advanced Networking Applications (IJANA)

[2]. B. Sosinsky, Cloud Computing Bible: Wiley, 2011.

[3]. MEHMUD ABLIZ Department of Computer Science, University of Pittsburgh- "Internet Denial of Service Attacks and Defense Mechanisms".

[4]. Anup Bhange, Amber Syad, Satyendra Singh Thakur- "DDoS Attacks Impact on Network Traffic and its Detection Approach" , International Journal of Computer Applications (0975 – 8887) Volume 40– No.11, February 2012.

[5]. C. Yu, H. Kai, and K. Wei-Shinn, "Collaborative Detection of DDoS Attacks over Multiple Network Domains," IEEE Transactions on Parallel and Distributed Systems, vol. 18, no. 12, pp. 1649-1662, 2007.

[6]. J. Mirkovic, G. Prier, and P. Reiher, "Source-end DDoS defense," in Second IEEE International Symposium on Network Computing and Applications, 2003, pp. 171-178.

[7]. Z. Yi, L. Qiang, and Z. Guofeng, "A real-time DDoS attack detection and prevention system based on per-IP traffic behavioral analysis," in 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), Chengdu, 2010, pp. 163-167.

[8]. N. Mitrou, K. Kontovasilis, G. Rouskas, I. Iliadis, L. Merakos, T. Peng, C. Leckie, and K. Ramamohanarao, "Proactively Detecting Distributed Denial of Service Attacks Using Source IP Address Monitoring," in Networking 2004. vol. 3042: Springer Berlin Heidelberg, 2004, pp. 771-782.

[9]. J. Rasool, I.-M. Fatemeh, A. Morteza, and S. Hamid Reza, "Detection of distributed denial of service attacks using statistical pre-processor and unsupervised neural networks," in Proceedings of the First international conference on Information Security Practice and Experience Singapore: Springer-Verlag, 2005, pp. 192-203.

[10]. S. N. Shiaeles, V. Katos, A. S. Karakos, and B. K. Papadopoulos, "Real time DDoS detection using fuzzy estimators," Computers & Security, vol. 31, no. 6, pp. 782-790, 2012.

[11]. W. Yi-Chi, T. Huei-Ru, Y. Wuu, and J. Rong-Hong, "DDoS Detection and Traceback with Decision Tree and Grey Relational Analysis," in Third International Conference on Multimedia and Ubiquitous Engineering, Qingdao, 2009, pp. 306-314.

[12]. M. G. Thomer and P. Massimiliano, "MULTOPS: a data-structure for bandwidth attack detection," in Proceedings of the 10th conference on USENIX Security Symposium. vol. 10 Washington, D.C.: USENIX Association, 2001.

[13]. R. Thomas, Z. Hong, T. Huck, and T. Johnson, "NetBouncer: client-legitimacy-based high-performance DDoS filtering," in Proceedings of the DARPA Information Survivability Conference and Exposition 2003, pp. 14-25.

[14]. W. Jie, R. C. W. Phan, J. N. Whitley, and D. J. Parish, "Augmented Attack Tree Modeling of Distributed Denial of Services and Tree Based Attack Detection Method," in IEEE 10th International Conference on Computer and Information Technology (CIT) Bradford, 2010, pp. 1009-1014.

[15]. L. Limwiwatkul and A. Rungsawang, "Distributed denial of service detection using TCP/IP header and traffic measurement analysis," in IEEE International Symposium on Communications and Information Technology, Sapporo, Japan, 2004, pp. 605-610

[16.] C. Zhongqiang, C. Zhongrong, and D. Alex, "An Inline Detection and Prevention Framework for Distributed Denial of Service Attacks," The Computer Journal, vol. 50, no. 1, pp. 7-40, 2007.

[17]. H. Rahmani, N. Sahli, and F. Kammoun, "Joint Entropy Analysis Model for DDoS Attack Detection," in Fifth International Conference on Information Assurance and Security, Xian, 2009, pp. 267-271.

[18]. X. Yang, L. Ke, and Z. Wanlei, "Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics," IEEE Transactions on Information Forensics and Security, vol. 6, no. 2, pp. 426-437, 2011.

[19]. J. Francois, I. Aib, and R. Boutaba, "FireCol: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks," IEEE/ACM Transactions on Networking, vol. 20, no. 6, pp. 1828-1841, 2012.